ProofPOINTS
i360Gov's Tech Survey Results
IT SURVEY REPORT | APRIL 2012

Survey Results

Tracking the Use of Mobile Technologies in Government

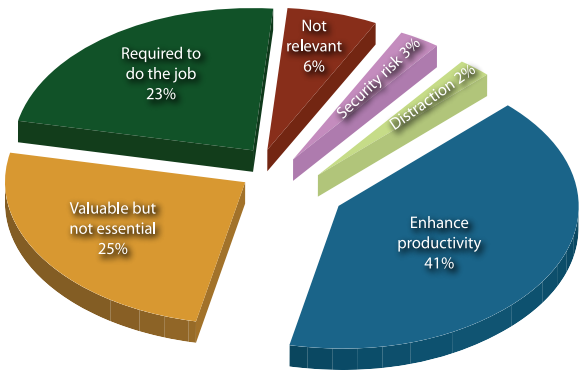
A desire to increase productivity, improve contact within agencies, along with enhancing the flexibility of working conditions, were cited by government executives as the three most compelling reasons to implement greater use of mobile devices, according to the results of a newly published i360Gov survey.

In an effort to track the growing use of mobile devices at all levels of public sector organizations, an online survey sponsored by SAP and Carahsoft, was conducted by i360Gov Custom Research, in February. In total, 331 government executives responded, providing invaluable insight on the acceptance and use of mobile technologies throughout all levels of government.

The survey of government executives found that 135 (41%) believe smartphones and other mobile devices enhance their productivity. Another 83 respondents (25%) said mobile devices were valuable, but not essential tools. And 75 more executives (23%) said that mobile devices are required to do their jobs. At the other end of the spectrum, few respondents expressed negative reactions to mobile technologies. For instance, 21 respondents (6%) said mobile devices are not relevant to their organization's mission or operations. Another nine respondents said the devices pose a security risk the organization is unwilling to accept. And eight executives surveyed (2%) called mobile devices a distraction that hurts productivity.

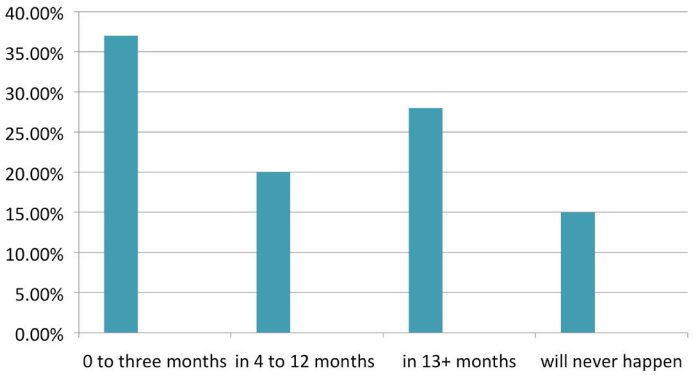
When asked about the percentage of the organization's employees who spend more than half of their time working/traveling outside of the office, a majority of respondents, 211 (64%) said 30% or fewer of the organization's employees work outside the office more than half of the time. Also, when asked about the percentage of employees that use mobile devices to do their jobs, again the largest number of respondents, 200 (60%) said less than 30% use smartphones, tablets or other mobile devices to complete daily tasks for work.

Mobile Devices: Tool or Distraction?



Source: i360Gov Custom Research

Plans to deploy mobile apps for employee use vary greatly



Source: i360Gov Custom Research

Interestingly, survey questions related to potential mobility plans garnered the greatest number of diametrically opposing opinions, either enthusiastically in favor or completely opposed to mobile technologies in government. For instance, when asked about the current stage of mobile device deployment, the largest number of those surveyed, 122 (37%) said they were already using mobile technologies. The second largest number of respondents, however, 62 (19%) said they are not considering mobility solutions at this time. Similarly, in a separate question on the timing of plans to implement mobile applications for citizen engagement, the largest number of respondents, 114 (34%) said it will take 13+ months for such a deployment to start. And the second largest number of respondents, 84 (25%) said such a deployment will never happen. Meanwhile, at the other end of the spectrum, 81 respondents, (24%) expect to start such a deployment within six months.

Finally, when asked about plans for the deployment of mobile applications for employees or internal use, the largest number, 123 (37%) said such plans are either under way or coming within three months. However, another 93 respondents (28%) said such plans are at least

13+months away, and 50 of those surveyed (15%) said such plans will never happen.

Even on the increasingly popular concept of 'bring your own device' (BYOD) for government work, responses varied widely. A total of 122 respondents (37%) said BYOD will never be allowed to happen within their organizations, while 118 respondents (36%) said their organizations already currently support employee-owned mobile devices at work.

By the end of 2013, government executives said the three most popular smartphone OS platforms that are likely to be supported within government organizations include: Blackberry OS, cited by 136 respondents (41%); Apple iOS, mentioned by 133 respondents (40%); and Android, selected by 100 respondents (30%). Another 111 (33%) were unsure which platforms would be supported. And Microsoft's Windows Mobile as mentioned by 60 respondents (18%). Survey respondents were asked to select all OS platforms that apply in their responses to this question.

The types of security policies used to protect mobile device use varied, with 171 (52%) of survey respondents having implemented passwords, along with inactivity timeouts. Another 72 or (22%) said the organization has implemented only password protection so far. And 78 respondents (24%) were either unsure, or believed there was as of yet no clear security policy in place to secure mobile device use.

The survey was conducted online, via email, during January and early February 2012. In terms of demographics, the largest number of respondents, 117 (35%) said they worked in executive/senior management within their division, agency or departments, while another 60 executives (18%) identified themselves as 'C' level executives (Chief, CIO, CSO, COO, CEO, CFO, etc.). Approximately 10% of respondents worked in program/project management. And at the same time, 43 executives (13%) filled administrative/operations management posts.

On the Cusp of Transformation: Awaiting a Federal Mobility Roadmap

Greater Guidance Needed to Help Agencies Securely Manage Mobility

The growing influx of mobile devices into all aspects of daily life has driven federal oversight organizations to launch a new strategy to allow for greater mobility throughout all levels of government, though further guidance is needed to help organizations securely embrace mobile devices for daily operational use.

The Federal Mobility Strategy launched in early 2012 was structured to help accelerate the government's adoption of mobile technologies and services by:

- Improving delivery of government information, products and services;
- Engaging citizens more fully and meaningfully with government;
- Reducing the cost of government operations through technology-enabled efficiencies; and
- Increasing productivity by freeing government employees and contractors from outdated work practices.

At the time of the strategy's launch, Federal CIO Steven Van Roekel said that by 2013, "I expect the government to change the way we work — to start embracing mobility-enabling technology across the federal workforce in a coordinated way and to start working on plans to deliver mobile-accessible content and services to the American people."

Greater government-wide acceptance of mobile technologies would mesh well with current industry estimates indicating the number of the smartphone customers is expected to reach one billion by 2016. At the same time, results from i360Gov's recent online survey of 331 government executives underscores strong interest in all things mobile, along with opposing opinions about what is considered acceptable when it comes to mobile device use in government.

Clearly, i360Gov's survey results indicate that government executives are unsure about how to allow greater mobility without risking security breaches. As with any relatively new initiative, there's still much confusion and government entities at all levels are looking forward to specific guidance to be issued by Federal CIO Van Roekel in the coming months.

In the meantime, innovative use cases have emerged, including one at USAID, which has issued a variety of mobile devices for use by field officers around the globe. And the Veterans Administration (VA), in an effort to stay current with private sector healthcare settings has provided tablets for VA physicians to use in tracking patient encounters. In another example, the Air Force purchased a large number of iPads for training, maintenance and operations staff to use on flight decks. And the U.S. Census mobilized more than 140,000 devices in its latest census effort. "At this early stage, the trend in government has been to focus primarily on field workers, not a government organization's entire workforce," said Lauren Jones, senior principal analyst for Deltek's Federal Market Analysis program.

Whether agencies lead or lag at this early stage of market acceptance, there's a strong requirement to lay a foundation for greater mobility. Clearly, the use of mobile devices has altered how most people do many things every day. "There has been a huge shift in the way we interact via mobile technology. It has become a habit many of us leverage for multiple reasons," said Dante Ricci, Director, SAP Public Sector Innovation.

The government's evolving digital government strategy should include a cohesive mobility roadmap to help agencies promote efficiency, manage IT costs and risks, and extend operations and analytics to the world of mobile devices, Ricci explained. "Agency-wide mobility initiatives will induce new, more productive work habits," said Ricci, eliminating archaic process steps and providing on-device access to information anytime, anywhere.

Advice For Embracing Mobility

As government organizations at all levels await better guidance, there is a good deal of practical advice already available to help them securely embrace mobility for employees, constituents and other stakeholders.

The National Institute of Standards and Technology (NIST) will issue published guidance on mobile device security this summer with the fourth revision of its Security and Privacy Controls for Federal Information Systems and Organizations, (Special Publication 800-53). According to Tom Karygiannis, a NIST Senior Researcher, the new guidance will be designed to explain potential threats and operational, management and technical countermeasures available for agencies to choose from. However, each agency must still perform "their own risk analysis and evaluation of the countermeasures most suitable for their enterprise," he explained.

For example, Karygiannis continued, allowing employees to bring their own devices to work is a policy decision to be resolved by agency top management. "Each agency must decide if the productivity gains or capabilities are worth the associated risk," he said.

For now, NIST recommends if an agency has determined the information mobile devices will hold, process or transmit requires the use of cryptography to protect the confidentiality, availability or integrity of that information, then those mobile devices are required to employ cryptography validated to meet Federal Information Processing Standards FIPS 140-2. NIST, through its Cryptographic Module Validation Program (CMVP), validates that the cryptographic modules used by, or in, each device meet the requirements of FIPS 140-2. Part of the E-Gov Act of 2002, FIPS 140-2 is a federal security standard authorized by the U.S. Secretary of Commerce. NIST officials stressed the organization's role isn't to create government regulations. And NIST also doesn't test products or approve mobile devices for use by federal agencies. Instead, NIST's role is to validate that the cryptography used is employed correctly.

Ultimately, despite ongoing confusion and potential security risks, government agencies must work out a way to allow greater mobility for workers, constituents and stakeholders. Of course, security is of paramount importance, and goes beyond passwords. "Agencies must use a multi-layered approach to protect against data loss or breaches," said Jones.

Because sometimes smartphones and notebook computers get lost and/or stolen, each device must be able to be remotely wiped clean. And identity management controls must be implemented to ensure users are properly authorized to access government resources. Most importantly, Jones advises government organizations to avoid approaching mobile device use on an 'ad-hoc' basis. "Organizations at all levels of government really need to develop a comprehensive strategy for mobility," she said.

A comprehensive strategy would hone in on each organization's mission, how employees work, how and where a mobile strategy would complement the organization's Continuity of Operations Plans (COOP). "Building a comprehensive mobility strategy, with proper security and governance built-in, is the best way to reduce potential risks," Jones said.

A key area of focus to include in agency mobility strategies should be sourcing. "So far, most purchasing has been completed on an 'as-needed' basis, and some agencies have, as a result, paid more than they should," Jones explained. Agencies should use strategic sourcing

methods to procure mobile solutions, and strive to reduce the total number of devices issued to employees.

Ultimately, mobility truly is part of a broader end-user productivity strategy, Jones explained, echoing what Van Roekel and others involved in federal oversight have said. Agencies must decide the conditions under which it makes sense for workers to have laptops, versus desktops, or tablets or smart phones, she continued. There's strong requirement to focus on agency-specific job tasks. "Are agency users creators or consumers of data? Are they power users who will need the bigger, better tools? Will the organization allow employees to bring their own, via BYOD?" she asked.

In an era of greater transparency and accountability -- along with tight budgets -- a government mobility really makes sense. Increased federal reporting requirements will encourage agencies to think more strategically, keep track of devices for mobile expense management, and for required reporting on energy use/compliance. According to Jones, "as agencies are forced to justify their actions, incorporate more metrics to measure performance, all signs indicate that agencies will need a comprehensive mobility strategy to address how they acquire, issue and secure mobile devices, along with how well they manage those expenses over time."

Mobile Security Considerations

A secure mobility strategy must include:

Network Security -- activities such as wireless e-mail can present a threat. This is why precautions are required to ensure no unsecured personal devices are allowed access to government networks, which could otherwise lead to viral infections of wired and wireless endpoints as well as the network.

Device Security -- government data on personal devices is at risk of theft or misplacement. Security measures include mobile information protection and control for data loss prevention and file encryption, mobile security and vulnerability management for device lockdown, security policy and compliance management, and mobile anti-malware to establish firewalls to protect against viruses and intrusion.

Identity Security -- identity information is also at risk from snooping. A strong reliance on authentication and authorization through mobile identity and access management is required to protect/authenticate mobile device users.

Source: SAP